MATH 101A: ALGEBRA I
PART B: RINGS AND MODULES

In the unit on rings, I explained category theory and general rings at the same time. Then I talked mostly about commutative rings. In the unit on modules, I again mixed category theory into the basic notions and progressed to the structure theorem for finitely generated modules over PID's. Jordan canonical forms were used as an application. The uniqueness part of the structure theorem was put off for the discussion on tensor product in Part C.

Contents

1. Basic definitions

In the first week, I reviewed the basic definitions and rephrased them in a categorical framework. The purpose of this was two-fold. First, I wanted to make the preliminaries more interesting for those of you who already know the basic concepts. Second, I want students to feel more comfortable with category theory so that I can use it later to explain more difficult concepts.

1.1. **Rings and endomorphisms.** First of all, an *additive group* is defined to be an abelian group in which the composition law is written as addition and the neutral element is called "0". When the group law is written as multiplication, it is called a *multiplicative group* whether or not it is abelian.

Definition 1.1. A *ring* is an additive group R together with a biadditive, associative multiplication law with unity. More precisely, a ring is: $(R, +, \cdot, 0, 1)$ where

(1) $(R, +, 0)$ is an additive group.
(2) $(R, \cdot, 1)$ is a monoid. I.e., multiplication is associative and has unit 1.
(3) Multiplication distributes over addition from the left and the right. I.e.,

$$a(b+c) = ab + ac \qquad (a+b)c = ac + bc$$

This condition is called *bi-additivity* since the multiplication mapping $(x, y) \mapsto xy$ is additive (a homomorphism) in each variable.

Lang allows $1 = 0$. I don't. But there is only one ring with this property, namely the zero ring, since any ring with $1 = 0$ has the property that

$$x = 1x = 0x = 0$$

for all $x \in R$.

To make a category we need homomorphisms.

Definition 1.2. If R, S are rings, a *ring homomorphism* $\phi : R \to S$ is a set mapping which is

(1) additive: $\phi(r + s) = \phi(r) + \phi(s)$
(2) multiplicative: $\phi(rs) = \phi(r)\phi(s)$
(3) unital: $\phi(1) = 1$.

I pointed out that the image of a ring homomorphism is a *subring* of S, i.e., a subset of S which is closed under addition, subtraction,

multiplication and contains 1. The *kernel* of ϕ is a (two-sided) *ideal* in R, i.e., a subset $I \subseteq R$ so that I is an additive subgroup of R and $RI = I = IR$.

One example of a ring is given by the endomorphism ring of any nonzero (!) additive group. If A, B are additive groups, then $\mathrm{Hom}_{\mathcal{A}dd}(A, B)$ is also an additive group where addition is defined pointwise:

$$(f + g)(x) = f(x) + g(x).$$

Here $\mathcal{A}dd$ is the category of additive groups and homomorphisms. In the case $A = B$, homomorphisms $f : A \to A$ are called *endomorphisms* of A and we write $\mathrm{End}(A) = \mathrm{Hom}(A, A)$. Being a Hom set, it is an additive group. But now we also have a composition law

$$\circ : \mathrm{End}(A) \times \mathrm{End}(A) \to \mathrm{End}(A).$$

The composition law distributes over addition on both sides for different reasons:

(1) Distributivity from the left comes from the fact that these are homomorphisms:

$$f(g + h)(x) = f(g(x) + h(x)) = fg(x) + fh(x) = (fg + fh)(x).$$

(2) Distributivity from the right comes from the definition of addition in $\mathrm{End}(A)$:

$$(f + g)h(x) = fh(x) + gh(x) = (fh + gh)(x).$$

Composition of mappings is always associative and the identity mapping acts as unity $id : A \to A$. Therefore, $(\mathrm{End}_{\mathcal{A}dd}(A), +, \circ, 0, id)$ is a ring (provided that $A \neq 0$).

The idea is that $\mathrm{End}(A)$ has addition and multiplication (given by composition) satisfying a list of conditions. *Rings* are subsets $R \subseteq \mathrm{End}(A)$ which has all of this structure. I.e., R is closed under addition, subtraction, multiplication and contains 0 and 1.

Question: If we start with a ring R then what is A?

Answer: We can take $A = (R, +)$, the underlying additive group of R. Then we have a ring monomorphism

$$\phi = \lambda : R \to \mathrm{End}(R, +)$$

given by $\phi(r) = \lambda_r$ which is left multiplication by r. This is an additive endomorphism of R by left distributivity:

$$\lambda_r(a + b) = r(a + b) = ra + rb = \lambda_r(a) + \lambda_r(b).$$

The additivity of the mapping $\phi = \lambda$ follows from right distributivity (in R):

$$\phi(r+s)(x) = \lambda_{r+s}(x) = (r+s)x = rx+sx = \lambda_r(x)+\lambda_s(x) = (\phi(r)+\phi(s))(x).$$

The fact that ϕ is multiplicative follows from the associativity of multiplication in R:

$$\phi(rs)(x) = (rs)x = r(sx) = \phi(r)\phi(s)(x).$$

The fact that ϕ is a monomorphism follows from the fact that 1 is a right unity:

$$(\forall x \in R)(\phi(r)(x) = 0) \Rightarrow \phi(r)(1) = r1 = r = 0.$$

The fact that $\phi(1) = 1$ follows from the fact that 1 is a left unity:

$$\phi(1)(x) = 1x = x.$$

Thus, all of the properties of a ring (the ones which involve the multiplication), are included in the statement that $\phi = \lambda : R \to \mathrm{End}(R, +)$ is a ring homomorphism.

1.2. **Modules.** When we think of R as being a subring of $\mathrm{End}_{\mathcal{A}dd}(A)$, the additive group A is called an R-module.

Definition 1.3. An *R-module* is an additive group M together with a ring homomorphism $\phi : R \to \mathrm{End}_{\mathcal{A}dd}(M)$.

This is usually stated in longhand as follows. For every $r \in R, x \in M$ there is $rx \in M$ with the following properties for all $r, s \in R$ and $x, y \in M$.

(1) $r(x + y) = rx + ry$ (I.e., $\phi(r)$ is additive, or equivalently, ϕ is a set mapping.)
(2) $(r + s)x = rx + sx$ (I.e., ϕ is additive.)
(3) $(rs)x = r(sx)$ (I.e., ϕ is multiplicative.)
(4) $1x = x$ (I.e., $\phi(1) = id = 1$.)

For example, R is an R-module and any left ideal in R is an R-module. (A *left ideal* is a proper additive subgroup $I \subset R$ so that $RI = I$.)

2. Examples

Today, I gave some examples of rings and functors associated to rings.

2.1. $\mathbb{Z}$, the integers.

The first example is $\mathbb{Z} = (\mathbb{Z}, +, \cdot, 0, 1)$. This is a ring which has the property of being the initial object in the category of rings. In other words, for any ring R there is a unique ring homomorphism

$$\phi : \mathbb{Z} \to R.$$

This is given by $\phi(1) = 1, \phi(2) = 1 + 1, \cdots$ and $\phi(-n) = -\phi(n)$. The uniqueness follows from the fact that $\mathbb{Z}$ is generated as an additive group by 1. So, ϕ is determined by what it does to 1 which is $\phi(1) = 1$ by definition of a ring homomorphism.

2.2. $U(R)$, the group of units.

Definition 2.1. A *unit* in a ring R is any invertible element. I.e., $x \in R$ is a unit if $xy = yx = 1$ for some $y \in R$. The units of a ring form a group called the *group of units* $U(R)$.

Proposition 2.2. *U is a functor from the category of rings to the category of groups.*

Proof. Any ring homomorphism $\phi : R \to S$ takes units to units since $xy = yx = 1$ implies

$$\phi(xy) = \phi(x)\phi(y) = \phi(yx) = \phi(y)\phi(x) = \phi(1) = 1.$$

□

In the next example, I constructed the adjoint of this functor.

2.3. group rings.

Suppose that G is a multiplicative group and R is a commutative ring. Then the *group ring* RG is defined to be the set of all finite linear combinations

$$\sum r_i g_i$$

where $r_i \in R, g_i \in G$ where we are allowed to simplify (i.e., there is an equivalence relation) using the relation

$$rg + sg = (r + s)g$$

whenever the g_i are not distinct.

Addition is defined by just putting the terms together. For example,

$$(ag_1 + bg_2) + (ch_1 + dh_2) = ag_1 + bg_2 + ch_1 + dh_2.$$

In Σ notation this is

$$\sum_{i=1}^{n} r_i g_i + \sum_{j=1}^{m} s_j h_j = \sum_{i=1}^{n+m} r_i g_i$$

where we use the s's and h's when the index i becomes too large. I.e., $r_{n+j} = s_j, g_{n+j} = h_j$.

Multiplication is given by

$$\left(\sum r_i g_j\right)\left(\sum s_j h_j\right) = \sum_{i,j} r_i s_j g_i h_j$$

Example 2.3. Suppose that $G = \langle t \,|\, t^3 \rangle$. This is the group generated by t modulo the relation $t^3 = 1$. So, $G = \{1, t, t^2\}$ is the multiplicative group which is isomorphic to the additive group $\mathbb{Z}/3\mathbb{Z}$. The group ring is

$$RG = \{a + bt + ct^2 \,|\, a, b, c \in R\}$$

Example 2.4. Let G be the infinite cyclic group $Z = \langle t \rangle = \{t^n \,|\, n \in \mathbb{Z}\}$. This is the multiplicative version of the additive group $\mathbb{Z}$. Then the group ring RZ is the ring of all *Laurent polynomials*

$$a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 + a_{-1} t^{-1} + \cdots + a_{-m} t^{-m}$$

where $a_i \in R$.

The usual notation for the Laurent polynomial ring is

$$R[t, t^{-1}] = RZ$$

Here, the square brackets indicate that this is the ring generated by R, t, t^{-1}. In general, if R is a subring of a ring S and $x_1, \cdots, x_n \in S$ then $R[x_1, \cdots, x_n]$ is defined to be the smallest subring of S containing R and the elements $x_1, \cdots, x_n$. (I.e., you just take the intersection of all such subrings.) This is in contrast to the round bracket notation which indicates a field. For example $\mathbb{Q}(t)$ is the smallest field containing $\mathbb{Q}$ and t.

Recall that a *field* is a commutative ring so that every nonzero element x has an inverse y ($xy = yx = 1$).

Proposition 2.5. *There is a bijection*

$$U(R) \cong \mathrm{Hom}_{Rings}(\mathbb{Z}[t, t^{-1}], R)$$

given by sending $x \in U(R)$ to the homomorphism $\phi : \mathbb{Z}[t, t^{-1}] \to R$ which sends $\sum n_i t^i$ to $\sum n_i x^i$. (This is called the evaluation map *since it sends a Laurent polynomial to its value at x.)*

Theorem 2.6. *The adjoint of the unit functor U is given by the integer group ring functor $\mathcal{G}ps \to \mathcal{R}ings$ which send G to $\mathbb{Z}G$. I.e.,*

$$\mathrm{Hom}_{\mathcal{G}ps}(G, U(R)) \cong \mathrm{Hom}_{Rings}(\mathbb{Z}G, R)$$

Proof. Suppose that $f : G \to U(R)$ is a group homomorphism. I.e., $f(gh) = f(g)f(h)$. Then we get a ring homomorphism $\phi : \mathbb{Z}G \to R$ by

$$\phi\left(\sum n_i g_i\right) = \sum n_i f(g_i)$$

This is additive by definition and multiplicative since f is multiplicative. Also $\phi(1) = f(1) = 1$. Conversely, G is contained in the group of units of $\mathbb{Z}G$. So, any ring homomorphism $\phi : \mathbb{Z}G \to R$ induces a group homomorphism

$$G \hookrightarrow U(\mathbb{Z}G) \xrightarrow{U\phi} U(R).$$

And it is easy to see that these constructions are inverse to each other and therefore give a bijection between $\mathrm{Hom}_{\mathcal{G}ps}(G, U(R))$ and $\mathrm{Hom}_{Rings}(\mathbb{Z}G, R)$. □

Corollary 2.7. *If there is an inverse system of rings, the units of the inverse limit are the inverse limit of the units:*

$$U(\lim R_i) \cong \lim U(R_i)$$

What follows is definitely not the best proof of this fact. However, it illustrates the use of category theory.

Proof. I used the theorem which gives a bijection. But the natural mapping is a homomorphism for the following reason. Given any diagram of rings R_i we get a diagram of groups $U(R_i)$ since U is a functor. The homomorphisms $\lim R_i \to R_i$ induce group homomorphisms $U(\lim R_i) \to U(R_i)$ which induces a group homomorphism

$$U(\lim R_i) \to \lim U(R_i).$$

I want to show that this is a bijection.

Now, use the natural bijections:

$$U(R_i) \cong \mathrm{Hom}_{\mathcal{G}ps}(Z, U(R_i)) \cong \mathrm{Hom}_{Rings}(\mathbb{Z}[t, t^{-1}], R_i)$$

Then the universality of the inverse limit can be stated as:

$$\mathrm{Hom}_{Rings}(X, \lim R_i) \cong \lim \mathrm{Hom}_{Rings}(X, R_i)$$

for all rings X. Apply this to $X = \mathbb{Z}[t, t^{-1}]$ gives

$$U(\lim R_i) \cong \lim U(R_i).$$

□

2.4. **matrix rings over fields.** Suppose that K is a field. Consider the set of $n \times n$ matrices with coefficients in K. We write $A = (a_{ij})$. Using the usual addition and multiplication of matrices:

$$(A + B)_{ij} = a_{ij} + b_{ij}$$

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

we get a ring $\mathcal{M}_n(K)$ called the $n \times n$ *matrix ring* over K.

I used this example to illustrate the concept of equivalence between rings and additive categories. When we take $n \times n$ matrices over K, there are some special matrices which have special significance. These are the idempotents, e.g.,

$$e_2 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

The definition is: $e \in R$ is an *idempotent* if $e^2 = e$. For matrices, the "primitive" idempotents are e_i the diagonal matrix with 1 in the ii position and 0 everywhere else. Two idempotents e_1, e_2 are called *orthogonal* if $e_1 e_2 = e_2 e_1 = 0$. (A *primitive* idempotent is one which cannot be written as a sum of orthogonal idempotents.) We can write unity I_n as a sum of n orthogonal idempotents:

$$1 = e_1 + e_2 + \cdots + e_n.$$

This is a maximal such decomposition. This is significant because of the following general construction.

2.5. **idempotents give a category.** Now suppose that R is any ring and

$$1 = e_1 + e_2 + \cdots + e_n$$

is a decomposition of unity into orthogonal idempotents. Then we can construct a category $\mathcal{C}$ as follows. The objects of $\mathcal{C}$ are the idempotents $e_1, \cdots, e_n$ and the morphism sets are the sets

$$\mathrm{Hom}_{\mathcal{C}}(e_i, e_j) := e_j R e_i.$$

Note that this is a additive group. In fact, aRb is an additive group for any $a, b \in R$ since it is closed under addition:

$$arb + asb = a(r + s)b \in aRb$$

and negation:

$$-arb = a(-r)b \in aRb$$

and contains $0 = a0b$.

Composition is defined by multiplication:

$$(e_k s e_j) \circ (e_j r e_i) := (e_k s e_j)(e_j r e_i) = e_k s e_j r e_i$$

Note that, since multiplication is biadditive, composition gives a biadditive mapping

$$\mathrm{Hom}_{\mathcal{C}}(e_j, e_k) \times \mathrm{Hom}_{\mathcal{C}}(e_i, e_j) \to \mathrm{Hom}_{\mathcal{C}}(e_i, e_k)$$

The identity morphism of e_i is

$$e_i = e_i 1 e_i \in \mathrm{Hom}_{\mathcal{C}}(e_i, e_i) = e_i R e_i$$

It is easy to check that this is the identity morphism:

$$(e_j r e_i) e_i = e_j r e_i = e_j (e_j r e_i)$$

So, we have a category. This category has additional structure since the Hom sets are additive groups and composition is biadditive. A category with this kind of structure is called a *pre-additive category*. (It would be an *additive category* if it also had a zero object and was closed under finite products and/or finite coproducts. (They are equivalent in a pre-additive category.)

3. Commutative rings: basics

I went over the basic facts about ideals in commutative rings.

3.1. **maximal ideals.**

Definition 3.1. A *maximal ideal* in a ring R is an ideal which is not properly contained in any other ideal.

Zorn's lemma tells us that all rings have maximal ideals.

Theorem 3.2. *Any ideal I in any ring R is contained in a maximal ideal. In particular, R has at least one maximal ideal.*

Proof. To prove this we need:

Axiom 3.3 (Zorn's Lemma)**.** *If P is a partially ordered set in which every tower has an upper bound, then P has a maximal element.*

Partially ordered means it has a transitive, reflexive, antisymmetric relation $\leq$ (so that $a \leq b, b \leq a \Rightarrow a = b$). In this case we are talking about the set of all ideals $J \subset R$ which contain I. A *tower* is a totally ordered subset: i.e., $T = \{J_\alpha\}$ is a tower if for all α, β either $J_\alpha \subseteq J_\beta$ or $J_\beta \subseteq J_\alpha$. If we had such a tower, the union

$$J_\infty = \bigcup J_\alpha$$

is an ideal containing every J_α and not containing 1. Since J_∞ contains each J_α, J_∞ is an upper bound for the tower. So, Zorn's lemma tells us that there is a maximal element in the poset of all ideals containing I. I.e., I is contained in a maximal ideal. □

Lemma 3.4. *A commutative ring is a field if and only if* 0 *is the only ideal.*

Proof. If R is a not a field then it has an element $x \neq 0$ which is not invertible. Then $(x) = xR$ is a nonzero ideal. The converse is obvious. □

Proposition 3.5. *An ideal I is maximal if and only if R/I is a field.*

Proof. The ideals of R/I all have the form J/I where J is an intermediate ideal, i.e., $I \subseteq J \subset R$. So, I is maximal iff $I/I = 0$ is a maximal ideal in R/I iff R/I is a field. □

3.2. **zero divisors and prime ideals.**

Definition 3.6. An ideal P is called *prime* if the complement of P is closed under multiplication, i.e., $a, b \notin P \Rightarrow ab \notin P$.

Definition 3.7. A *zero divisor* is a nonzero element $a \in R$ so that $ab = 0$ for some $b \neq 0$ in R. A ring with no zero divisors is called a *domain* (or *integral domain*). Lang uses the adjective *entire* for this. I.e., a domain is an entire ring.

Example 3.8. If R, S are commutative rings then the Cartesian product $R \times S = \{(r, s) \,|\, r \in R, s \in S\}$ is a ring with addition and multiplication defined "coordinatewise":

$$(r, s) + (r', s') = (r + r', s + s')$$

$$(r, s)(r', s') = (rr', ss')$$

This ring has two idempotents:

$$e_1 = (1, 0), \qquad e_2 = (0, 1)$$

which are orthogonal: $e_1 e_2 = (0, 0) = 0$. These are zero divisors. If a ring has no zero divisors then it does not factor as a product! So, it is "one piece."

Having no zero divisors is the same as saying that the set of nonzero elements if closed under multiplication. This gives the following.

Proposition 3.9. *R is a domain if and only if 0 is a prime ideal.*

Corollary 3.10. *An ideal I in R is prime if and only if R/I is a domain.*

3.3. **polynomial rings.** If A is any ring, the *polynomial ring* $A[X]$ is defined to be the set of all formal expressions called *polynomials*:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

where $a_i \in A$. The word "formal expression" means that two such elements are equal if and only if they have the same coefficients a_i. Every polynomial gives a function $R \to R$ given by evaluation. But two polynomials might give the same function!

Suppose that A is a subring of B and $b \in B$. Then the *evaluation map*

$$ev_b : A[X] \to B$$

is the ring homomorphism given by

$$ev_b(f) = f(b) = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0.$$

More generally we have the ring of polynomials in several variables: $A[X_1, \cdots, X_n]$. This is defined recursively by

$$A[X_1, \cdots, X_n] = A[X_1, \cdots, X_{n-1}][X_n]$$

In other words, a polynomial in the variables $X_1, \cdots, X_n$ is the same as a polynomial in X_n whose coefficients are polynomials in the first $n-1$ variables.

Polynomial rings satisfy the following universal property.

Proposition 3.11. *If A is a subring of B and $x_1, x_2, \cdots, x_n \in B$ then there is a unique ring homomorphism*

$$ev_{(x)} : A[X_1, \cdots, X_n] \to B$$

which is equal to the inclusion map on A and which sends X_i to x_i.

Proof. This is sort of obvious. The homomorphism must be the one which sends $f(X_1, \cdots, X_n)$ to $f(x_1, \cdots, x_n)$. □

3.4. **Example.** I talked about the example $\mathbb{Z}[\sqrt{-5}]$ without complete proofs. We need theorems about PID's and UFD's to do this.

First, I pointed out that if B is a domain then the kernel of any evaluation map

$$\phi = ev_b : A[X] \to B$$

must be a prime ideal. The image is, by definition, the ring $A[b]$.

I took as an example, $B = \mathbb{C}$, $A = \mathbb{Z}$ and $b = \sqrt{-5}$. The prime ideal in this case is the principal ideal

$$\ker \phi = (X^2 + 5).$$

The image is the ring $\mathbb{Z}[\sqrt{-5}]$. The elements of this ring are

$$a + b\sqrt{-5}$$

where $a, b \in \mathbb{Z}$. The proof is simple. The set of such elements forms a ring and it is clearly the smallest ring containing $\mathbb{Z}$ and $\sqrt{-5}$.

This ring is not a UFR (unique factorization domain) since

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

And it is not a PID since

$$(2, 1 + \sqrt{-5})$$

is not a principal ideal. I.e., it is not equal to (a) for any $a \in R = \mathbb{Z}[\sqrt{-5}]$.

The elements $2, 3, 1 \pm \sqrt{-5}$ are *irreducible* elements of the ring R. This means that for any factorization of these elements, one of the factors will always be a unit. E.g., $2 = ab$ implies either a or b is a unit. The word "irreducible" is used since "prime" is a property of ideals not of numbers.

4. Localization

Today I talked about localization. I explained the basic definitions, gave examples and I also tried to explain what the word "local" refers to. All rings are commutative here.

4.1. basic definitions.

Definition 4.1. A subset $S \subseteq R$ is called a *multiplicative set* if S is closed under multiplication, $0 \notin S$ and $1 \in S$.

Some people leave out the assumption that $1 \in S$. It is not necessary since you can always add 1 to the set (take the union with $\{1\}$).

Definition 4.2. If S is a multiplicative set in a ring R then $S^{-1}R$ is defined to be the set of equivalence classes of symbols $\frac{x}{a}$ where $x \in R, a \in S$ and

$$\frac{x}{a} \sim \frac{y}{b} \text{ if } (\exists t \in S)\ xbt = ayt$$

This is a clumsy equivalence relation. So, I reformulated it as follows. This equivalence relation is the transitive relation generated by the symmetric relation given by

$$\frac{x}{a} \approx \frac{tx}{ta} \quad (\forall t \in S)$$

The reason is that:

$$\frac{x}{a} \approx \frac{xbt}{abt} = \frac{ayt}{abt} \approx \frac{y}{b}$$

Proposition 4.3. *$S^{-1}R$ is a ring with addition and multiplication given by*

$$\frac{x}{a} + \frac{y}{b} = \frac{xb + ay}{ab}$$
$$\frac{x}{a} \cdot \frac{y}{b} = \frac{xy}{ab}$$

and $j(x) = \frac{x}{1}$ gives a ring homomorphism $j : R \to S^{-1}R$.

Proof. We need to show that addition and multiplication are well-defined. The rest is straightforward. To show that addition is well-defined, we can use the stronger relation $\approx$:

$$\frac{sx}{sa} + \frac{ty}{tb} = \frac{sxtb + saty}{satb} = \frac{(st)(xb + ay)}{(st)ab} \approx \frac{xb + ay}{ab}.$$

Similarly,

$$\frac{sx}{sa} \cdot \frac{ty}{tb} = \frac{sxty}{satb} = \frac{(st)(xy)}{(st)ab} \approx \frac{xy}{ab}.$$

So, multiplication is also well-defined. □

4.2. **examples.** I gave a bunch of examples but I delayed the explanations for the end of the lecture.

Example 1. $R = \mathbb{Z}$ with multiplicative set $S = \{n \in \mathbb{Z} \mid n \neq 0\}$. Then $S^{-1}\mathbb{Z} = \mathbb{Q}$.

This is a special case of the more general example:

Example 2. Suppose that R is any domain and $S = R\backslash\{0\}$. Then

$$Q(R) = S^{-1}R$$

is the *quotient field* or *field of fractions* of R. This is a field since the nonzero elements of R are invertible:

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

This example required a discussion about which elements are zero and which are 1.

Proposition 4.4. *An element $\frac{x}{s} \in S^{-1}R$ is equal to zero if and only if there is an element $t \in S$ so that $xt = 0$.*

Proof. If such a t exists then

$$\frac{x}{s} \approx \frac{xt}{st} = \frac{0}{st} \sim \frac{0}{1} = j(0)$$

since $0 \cdot 1 = 0 = st \cdot 0$. Conversely, if

$$\frac{x}{s} \sim \frac{0}{1} = j(0)$$

then there is a $t \in S$ so that $xt = x1t = st0 = 0$. □

I forgot to do the same discussion with 1.

Proposition 4.5. *An element $\frac{x}{s} \in S^{-1}R$ is equal to $1 = \frac{1}{1} = j(1)$ if and only if there exists $t \in S$ so that $tx = ts$.*

Proof. This is just the definition of the equivalence relation. □

Example 3. Let $R = C^0(\mathbb{R})$. This is the ring of continuous functions $f : \mathbb{R} \to \mathbb{R}$ with the usual pointwise addition and multiplication. Let S be the set of all functions f which are nonzero at 1:

$$S = \{f \mid f(1) \neq 0\}$$

Then S is clearly a multiplicative set. I claim that $S^{-1}R$ is a "local ring" which means that the nonunits form an ideal. A fraction $f(x)/g(x)$ is an element of $S^{-1}R$ if $g(1) \neq 0$. It is invertible if $f(1) \neq 0$. So the

nonunits are given by the equation $f(1) = 0$ which clearly defines an ideal. In fact it is the kernel of the evaluation map

$$ev_1 : S^{-1}R \to \mathbb{R}.$$

This is a special case of the following more general example.

Example 4. If $P \subseteq R$ is a prime ideal then its complement $S = R \backslash P$ is a multiplicative set. (In fact these conditions are equivalent.) So, we can form the ring $S^{-1}R$ which is called the *localization* of R at P and written R_P.

Another special case of this is the following.

Example 5. Suppose that $p \in \mathbb{Z}$ is irreducible (i.e. a prime number). Then (p) is a prime ideal and we can form the localization:

$$\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \in \mathbb{Q} \,|\, p \not| \, b \right\}$$

This is a subring of $\mathbb{Q}$.

What is the relationship between $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p$?

4.3. **universal property.** In your homework you proved that if any integer n which is not divisible by p is uniquely invertible in $\mathbb{Z}_p$. Therefore, by the following universal property of the localization, there is a ring homomorphism

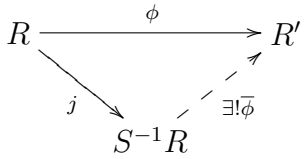
$$\mathbb{Z}_{(p)} \to \mathbb{Z}_p.$$

Is it onto? Is it a monomorphism?

Theorem 4.6. *If $S \subset R$ is a multiplicative set then $S^{-1}R$ has the following universal property: Given any ring homomorphism*

$$\phi : R \to R'$$

so that $\phi(S) \subseteq U(R')$ then there exists a unique ring homomorphism $\overline{\phi} : S^{-1}R \to R'$ so that $\overline{\phi} \circ j = \phi$. I.e., the following diagram commutes.



Proof. (Existence) The ring homomorphism $\overline{\phi}$ is given by $\overline{\phi}(x/s) = \phi(x)\phi(s)^{-1}$. You actually need to show that this is a homomorphism. This follows from the fact that the definition of addition and multiplication in $S^{-1}R$ used the rules which hold for arbitrary elements of the form xs^{-1}.

(Uniqueness) Suppose that $\psi : S^{-1}R \to R'$ is a homomorphism which extends j. Then the equation

$$\frac{x}{s} = \frac{x}{1} \cdot \frac{1}{s}$$

gives the equation

$$\psi\left(\frac{x}{s}\right) = \psi\left(\frac{x}{1}\right)\psi\left(\frac{1}{s}\right) = \phi(x)\phi(s)^{-1}$$

where $\psi(1/s) = \psi(s)^{-1} = \phi(s)^{-1}$ since ψ induces a group homomorphism

$$U(\psi) : U(R) \to U(R').$$

□

4.4. **local rings.** Localization is used to produce local rings.

Definition 4.7. A *local ring* is a ring R with a unique maximal ideal $\mathfrak{m}$.

Proposition 4.8. *A ring R is local if and only if the complement $R\backslash U(R)$ of the set of units is an ideal.*

The proof used the followings two obvious properties of $U(R)$.

Lemma 4.9. *An ideal in R cannot contain any units.*

This implies that any ideal is contained in $R\backslash U(R)$. So, if this is an ideal, it must be maximal.

Lemma 4.10. *Any element $a \in R$ which is not a unit generates an ideal (a).*

So, if there is only one maximal ideal, it contains all such a. So, $\mathfrak{m} = R\backslash U(R)$.

The term "localization" is justified by the following theorem which I forgot to prove. So, you can do it for homework.

Theorem 4.11. *If P is a prime ideal in R then R_P is a local ring.*

What I did explain is what the "local" means, at least topologically.

4.5. **germs of functions.**

Definition 4.12. Suppose that X, Y are topological spaces and $f : X \to Y$ is a mapping. Let $x_0 \in X$. Then the *germ* of f at x_0 is defined to be the equivalence class of f under the equivalence relation $f \sim g$ if there exists an open neighborhood U of x_0 in X so that

$$f|_U = g|_U$$

This is an equivalence relation since, if $g|_V = h|_V$, then

$$f|_{U\cap V} = g|_{U\cap V} = h|_{U\cap V}$$

and $U \cap V$ is an open neighborhood of x_0. Note that f need only be defined in a neighborhood of x_0.

When the target Y is a ring, the set of map germs forms a ring. If we put some restriction on the functions f (e.g., continuous, differentiable, polynomial), we get a subring. For example, we have a ring of germs at 1 of continuous functions $\mathbb{R} \to \mathbb{R}$. The notation is with a comma:

$$gr_1(f) : \mathbb{R}, 1 \to \mathbb{R}$$

In Example 3, we localized the ring of continuous functions $\mathbb{R} \to \mathbb{R}$ at the maximal ideal $S = \{f \mid f(1) \neq 0\}$ (making it into the unique maximal ideal). Two functions f, g give the same map germ at 1 if there exists an $\epsilon > 0$ so that

$$f(x) = g(x) \quad \forall x \in (1-\epsilon, 1+\epsilon)$$

In other words, the functions f, g agree in the ϵ neighborhood of 1 and the germs is just the function restricted to this arbitrarily small interval about 1.

The following theorem represents the intuitive concept that "localization" refers to restricting attention to a neighborhood of a point.

Theorem 4.13. *If $S = \{f \mid f(1) \neq 0\}$ then $S^{-1}C^0(\mathbb{R})$ is isomorphic to the ring of germs at 1 of continuous functions $\mathbb{R}, 1 \to \mathbb{R}$.*

Proof. Let G be the ring of germs at 1 of continuous functions $\mathbb{R}, 1 \to \mathbb{R}$. By definition, we have an epimorphism of rings

$$gr_1 : C^0(\mathbb{R}) \to G$$

For any $f \in S$, there is an $\epsilon > 0$ so that $f(x) \neq 0$ for all $x \in (1-\epsilon, 1+\epsilon)$. Let $g : \mathbb{R} \to \mathbb{R}$ be given by

$$g(x) = \begin{cases} 1/f(x) & \text{if } |x-1| \leq \epsilon/2 \\ 1/f(1-\epsilon/2) & \text{if } x \leq 1-\epsilon/2 \\ 1/f(1+\epsilon/2) & \text{if } x \geq 1+\epsilon/2 \end{cases}$$

This is a continuous function so that the product $f \cdot g$ is equal to 1 in a neighborhood of 1. Therefore, $gr_1(f)$ is invertible in the ring of germs. So, by the universal property we have a ring homomorphism

$$\overline{gr}_1 : S^{-1}C^0(\mathbb{R}) \to G$$

which is surjective. So, we just have to show that the kernel is zero.

Suppose that $f/g \in \ker \overline{gr}_1$. Then, for some $\epsilon > 0$,

$$f(x)/g(x) = 0 \quad \forall x \in (1-\epsilon, 1+\epsilon).$$

But this implies that $f(x) = 0$ in that interval. Let $h : \mathbb{R} \to \mathbb{R}$ be a continuous function so that $h(1) \neq 0$ but $h(x) = 0$ whenever $|x-1| \geq \epsilon$. (For example, $h(x) = \max(0, \epsilon - |x-1|)$.) Then the product $f \cdot h = 0$ and in $S^{-1}C^0(\mathbb{R})$ we have

$$\frac{f}{g} = \frac{fh}{gh} = \frac{0}{gh} = 0.$$

Therefore, $\overline{gr}_1$ is an isomorphism of rings. □

In algebraic geometry, we should take $\mathbb{C}$ instead of $\mathbb{R}$ and we should take the Zariski topology. The open subsets of $\mathbb{C}$ are then the complements of finite sets. We should take polynomial functions

$$\mathbb{C} \to \mathbb{C}$$

and invert the ones which are not zero at some point, say a. This is the complement of the maximal ideal $(X - a) \subset \mathbb{C}[X]$. Then we get the local ring

$$\mathbb{C}[X]_{(X-a)}$$

which is supposed to restrict attention to the behavior of polynomials at the point a.

5. Principal rings

(Lecture by Alex Charis, notes by Andrew Gainer)

Definition 5.1. Given a ring R, a *norm* is a function $N : R \to \mathbb{N} \cup \{0\}$ with $N(0) = 0$.

Definition 5.2. A domain R is a *Euclidean domain* if there is a norm on R such that, for all $a, b \in R$ with $b \neq 0$, there exists $q \in R$ so that $a = bq + r$ with $r = 0$ or $N(r) < N(b)$.

Example 5.3.
(1) $R = \mathbb{Z}$ with $N = |\cdot|$.
(2) $R = \mathbb{Z}[i]$ with $N = |\cdot|$.
(3) $R = F[x]$ with F a field and $N = deg$.

Definition 5.4. Let A be a domain. An element $a \in A$ with $a \neq 0$ is *irreducible* if $a = bc$ only if b or c is a unit in A.

Proposition 5.5. *Let $a \in A$ be such that $a \neq 0$ and (a) is prime. Then a is irreducible.*

Proof. Suppose $a = bc$. Then $bc \in (a)$. So, one is in the ideal. Suppose that $b \in (a)$. Then b is not a unit because $(a) \neq A$. But $b = ar$. So, $b = bcr$. Since A is a domain, $cr = 1$ and c is a unit as required. □

Definition 5.6. Let A be a domain and $a \in A$, $a \neq 0$. Then a is said to have a *unique factorization into irreducibles* if there exist a unit u and irreducibles p_i so that $a = up_1p_2 \cdots p_r$ and, if $a = vq_1 \cdots q_s$ for v a unit and q_i irreducible, then $s = r$ and $q_i = u_i p_i$ up to reordering.

Remark 5.7. • If p is irreducible and $u \in U(A)$, then up is irreducible.
• By convention, for $u \in U(A)$, $u = u$ is a factorization into irreducibles (with $r = 0$).

Definition 5.8. A domain A is a *unique factorization domain* (UFD) if every $a \in A$ with $a \neq 0$ has a unique factorization into irreducibles. Lang calls this a "factorial entire ring."

Definition 5.9. *a divides b* (denoted $a|b$) if there exists $c \in A$ so that $ac = b$.

Definition 5.10. If $d \in A$ such that $d \neq 0$ then d is a *greatest common divisor* (gcd) of a and b if $d|a, d|b$ and, if, for $e \neq 0$, $e|a, e|b$, then $e|d$.

Proposition 5.11. *If A is a PID and $a, b \in A$ with $a, b \neq 0$ then c is the gcd of a and b if $(a, b) = (a) + (b) = (c)$.*

Proof. Since $a, b \in (c)$ it is clear that $c|a$ and $c|b$. Since $c \in (a, b)$, we can write $c = va + sb$. So, if $d|a$ and $d|b$ then $c = vdx + sdy$ for some $x, y \in R$. So, $d|c$ as required. □

[I reversed the order in the notes and put uniqueness first:]

Lemma 5.12. *If A is a PID, p is irreducible in A and $a, b \in A$ with $p|ab$ then $p|a$ or $p|b$.*

Proof. Suppose $p \not| b$. Then $1 = gcd(p, b)$. So, $1 = px + qb$. So, $a = pax + qab$. So, $p|a$. □

This lemma implies the uniqueness of factorization in a PID. If $a = p_1 \cdots p_r = q_1 \cdots q_s$ then $p_1|a$ implies $p_1|q_i$ for some i. So, $q_i = up_1$. Then $up_2 \cdots p_r = q_1 \cdots \widehat{q_i} \cdots q_s$. By induction on r it follows that $r = s$ and the factorization is unique.

Theorem 5.13. *Let A be a PID. Then A is a UFD.*

Proof. Let S be the set of nonzero principal ideals whose generators do not have unique factorizations into irreducibles. Suppose $S \neq \emptyset$. Consider a chain $(a_1) \subsetneq (a_2) \subsetneq \cdots$ which is as long as possible (or infinite) and take its union. This union must be an ideal and is therefore principal. So, we call its generator a. Then $a \in (a_n)$. So, $(a) = (a_n)$ and the chain is finite. So, the generator of any ideal strictly containing (a) has a factorization.

Note that a cannot be irreducible (because then $a = a$ is a factorization). So, we can write $a = bc$ where b, c are not units. Then $(b) \supsetneq (a)$ and $(c) \supsetneq (a)$. So, b, c have factorizations. Then the product of these factorizes a and the factorization is unique by the lemma. So, $(a) \notin S$, a contradiction. So, $S = \emptyset$ which means that every nonzero element of A has a unique factorization. □

6. Modules: introduction

I talked about modules from scratch beginning with a repetition of the definition.

(1) definition
(2) examples
(3) free modules
(4) cyclic modules

6.1. **definition.**

Definition 6.1. A *(left) R-module* is an additive group M together with a ring homomorphism

$$\alpha : R \to \mathrm{End}(M).$$

The statement that α is a ring homomorphism is three statements:

(1) $\alpha(1) = 1$
(2) $\alpha(r+s) = \alpha(r) + \alpha(s)$
(3) $\alpha(rs) = \alpha(r)\alpha(s)$

Writing $\alpha(r)x = rx$ this list becomes:

(1) $1x = x$
(2) $(r+s)x = rx + sx$
(3) $(rs)x = r(s(x))$

6.2. **examples.**

Example 6.2. A left ideal $I \subset R$ is an R-module.

Example 6.3. The ring itself is a module. I.e., R is an R-module.

Example 6.4. The polynomial ring $R[X]$ is an R-module.

Example 6.5. If R is a field, an R-module is the same as a vector space V over the field R.

Definition 6.6. A *basis* for a vector space V over a field F is a subset $\mathcal{B} = \{b_i\} \subseteq V$ so that for every $v \in V$ there are unique scalars $x_i \in F$ almost all of which are zero so that $v = \sum x_i b_i$.

Theorem 6.7. *Every vector space V over a field K has a basis.*

We will prove this later. In fact, fields are PID's. So, this will be a special case of a more general theorem.

6.3. **free modules.**

Definition 6.8. An R-module M is *free* if it has a basis $\mathcal{B} = \{b_\alpha\}$. I.e., for every element x of M there are unique elements $r_i \in R$ almost all of which are zero so that

$$x = \sum r_i b_i.$$

Example 6.9. The product $R \times R \times R$ is free on the generators e_1, e_2, e_3.

Theorem 6.10. *Every module is a quotient of a free module.*

Proof. Let F be the free module generated by the set X of all nonzero elements of M. Then the inclusion map $X \to M$ induces an epimorphism $f : F \twoheadrightarrow M$ by the formula:

$$f\left(\sum r_i(x_i)\right) = \sum r_i x_i.$$

Here I used the notation (x_i) to denote the element of X corresponding to the element $x_i \in M$. This implies that M is isomorphic to the quotient:

$$M \cong F/\ker f.$$

□

This proof uses definitions which I was supposed to do earlier:

Definition 6.11. A *submodule* of an R-module M is defined to be an additive subgroup $N \subseteq M$ which is closed under the action of R. Thus:

(1) $0 \in N$
(2) $N + N = N$ (N is closed under addition: $N + N \subseteq N$. But this is equivalent to $N + N = N$ since $0 \in N$.)
(3) $RN = N$ (N is closed under multiplication by elements of R: $RN \subseteq N$. This is equivalent to $RN = N$ since $1 \in R$.)

Proposition 6.12. *If N is a submodule of M then the set of additive cosets:*

$$M/N := \{x + N \mid x \in M\}$$

forms an R-module.

Theorem 6.13. *If $f : M \to L$ is a homomorphism of R-modules then*

(1) $\ker f$ *is a submodule of* M.
(2) $\operatorname{im} f$ *is a submodule of* L.
(3) $\operatorname{im} f \cong M/\ker f$.

I gave an example of a module which is not free:

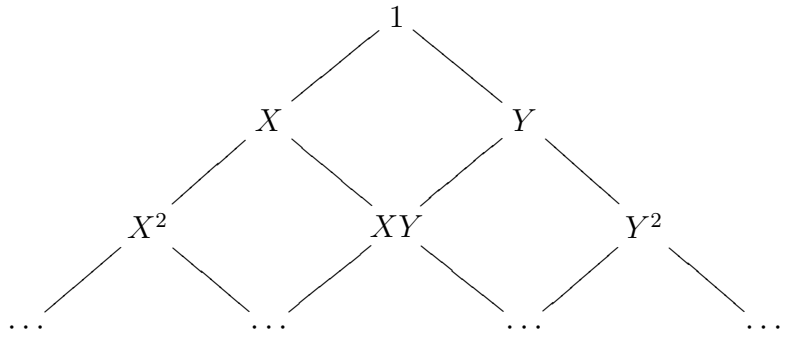
Example 6.14. Let $R = K[X, Y]$. Then the ideal (X, Y) is not a free module. It has generators X, Y but $Y(X) = X(Y)$. Another was to say this is that the epimorphism

$$R \times R \to (X, Y)$$

given by

$$(f, g) \mapsto Xf(X, Y) + Yg(X, Y)$$

is not an isomorphism since $(Y, -X)$ is in the kernel. I also drew a picture:



This is a visualization of a module because each monomial generates a submodule (ideal) and lines indicate containment, just as in a Hasse diagram.

6.4. **cyclic modules.**

Definition 6.15. A *cyclic module* is a module which is generated by one element. Thus $M = Rx$.

The question is: Can we describe all cyclic modules up to isomorphism?

If M is generated by the single element x then there is an epimorphism:

$$\phi : R \to M$$

given by $\phi(r) = rx$. This implies that $M \cong R/\ker\phi$. But what is the kernel of ϕ? It is by definition the set of all $r \in R$ so that $rx = 0$. This is called the *annihilator ideal* of x:

$$ann(x) := \{r \in R \,|\, rx = 0\}.$$

Thus,

$$M = Rx \cong R/ann(x).$$

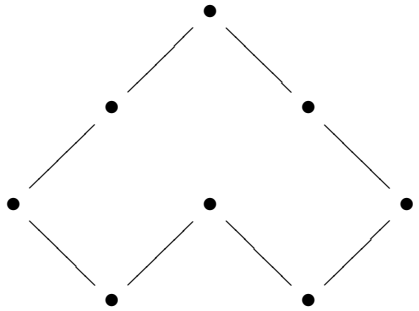
Conversely, given any left ideal $I \subseteq R$, the quotient R/I is a cyclic module. In order to give a complete classification of cyclic modules we still need to answer the following.

Question: Is it possible for two different ideals I, J to give isomorphic cyclic modules

$$R/I \cong R/J?$$

If so, we need to describe all the ideals J which give the same quotient up to isomorphism.

Cyclic modules can be visualized as a diagram with one peak:



For example, this could be $K[X,Y]/(X^3, X^2Y^2, Y^3)$. A finitely generated module could be visualized as a union of overlapping pictures of this kind.

[If someone can create the picture, I will insert it here.]

7. Products and coproducts

Today we talked about products and coproducts (sums) and some of the consequences of these concepts. We also talked about the difference. In particular, infinite products can be finitely generated but nontrivial infinite sums cannot.

(1) products
(2) sums
(3) projective modules
(4) finite generation

7.1. **products.** If $M_\alpha, \alpha \in I$, is a family of R-modules then we can form the Cartesian product

$$\prod_{\alpha \in I} M_\alpha = \{(x_\alpha) \,|\, x_\alpha \in M_\alpha\}$$

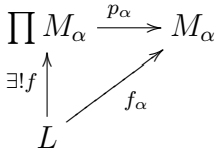
This is an R-module with addition and action of R given coordinate-wise. We have projection maps onto each coordinate:

$$p_\alpha : \prod_{\alpha \in I} M_\alpha \to M_\alpha$$

These are R-module homomorphisms.

Theorem 7.1. *The Cartesian product $\prod_{\alpha \in I} M_\alpha$ is the product in the category of R-modules.*

Proof. The statement is that, given any module L and homomorphisms $f_\alpha : L \to M_\alpha$, there exists a unique homomorphism $f = \prod f_\alpha : L \to \prod M_\alpha$ making the following diagram commute:



This is obviously true: f must send $x \in L$ to the unique element of $\prod M_\alpha$ whose α coordinate is $f_\alpha(x)$. □

7.2. **direct sums.** The direct sum is equal to the weak product:

$$\bigoplus_{\alpha \in I} M_\alpha = \prod_{\alpha \in I}{}' M_\alpha$$

where the weak product is the subset of the product consisting of elements where only finitely many coordinates are nonzero:

$$\prod{}' M_\alpha = \left\{(x_\alpha) \in \prod M_\alpha \,|\, x_\alpha = 0 \ \forall \forall \alpha\right\}$$

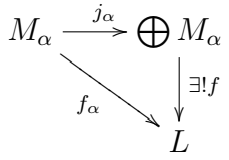
There are inclusion maps

$$j_\alpha : M_\alpha \to \bigoplus M_\alpha.$$

Every element of $\bigoplus M_\alpha$ is a sum of elements in the images of these inclusion maps.

Theorem 7.2. *The direct sum is the coproduct in the category of R-modules.*

Proof. Again, the main point is to understand the statement. The proof is trivial. This theorem says that, given any module L and homomorphisms $f_\alpha : M_\alpha \to L$, there is a unique morphism f from the direct sum to L making the following diagram commute.



The mapping f takes the element (x_α) to the sum $\sum f_\alpha(x_\alpha)$. This is defined since only finitely many of the coordinates x_α are nonzero. □

When the index set I is finite, the weak product is equal to the product. So, we get the following.

Corollary 7.3. *Given a finite collection of modules $M_1, \cdots, M_n$ the direct sum is equal to the direct product:*

$$\bigoplus_{i=1}^{n} M_i = \prod_{i=1}^{n} M_i.$$

The argument that proves that finite sums and products agree works in any preadditive category. Recall that a category $\mathcal{C}$ is *preadditive* if the Hom sets are additive groups and composition is biadditive.

Theorem 7.4. *If $M_1, \cdots, M_n$ are objects of any preadditive category, the finite product $\prod M_i$ exists in the category if and only if the finite sum (coproduct) $\bigoplus M_i$ exists in the category. Furthermore, they agree when they exist.*

Proof. Suppose the product $\prod M_i$ exists. Then, for each i, we have the identity map $id_{M_i} : M_i \to M_i$ and the zero maps $0 : M_i \to M_j$ when $i \neq j$. By the universal property of the product, this give a morphism

$$j_i = (0, 0, \cdots, 0, id_{M_i}, 0, \cdots, 0) : M_i \to \prod M_i$$

which has the property that

$$p_j \circ j_i = \delta_{ij}.$$

I.e., this is the identity if $i = j$ and zero if $i \neq j$. Given any object L of the category and morphisms $f_i : M_i \to L$, let $f : \prod M_i \to L$ be given by

$$f = \sum_{i=1}^{n} f_i \circ p_i.$$

Note that this uses only categorical properties: we can compose maps and we can add maps. Objects do not have elements! Since composition is biadditive we can make the following computation.

$$f \circ j_i = \sum_{j=1}^{n} f_j \circ p_j \circ j_i = \sum_{j=1}^{n} \delta_{ij} f_j = f_i$$

Thus f makes the diagram in the definition of the coproduct commute.

To prove the uniqueness of f we need the following equation which holds in the endomorphism group of $\prod M_i$.

$$\sum_{i=1}^{n} j_i \circ p_i = id.$$

To prove this, let h be the endomorphism given on the left. Then

$$p_j \circ h = \sum_{i=1}^{n} p_j \circ j_i \circ p_i = \sum_{i=1}^{n} \delta_{ij} p_i = p_j.$$

By the universal property of the product, this forces $h = id$.

Returning to the uniqueness of f. Suppose that $g : \prod M_i \to L$ is another morphism so that $g \circ j_i = f_i$. Then

$$(f - g) \circ j_i = f_i - f_i = 0.$$

So,

$$0 = (f - g) \circ \sum_{i=1}^{n} j_i \circ p_i = (f - g) \circ id = f - g$$

which implies that $f = g$. □

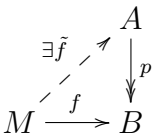
Definition 7.5. An *additive category* is a preadditive category which has finite products and sums including the empty sum which is the zero object. (Recall that a zero object is an object which is both initial and terminal.)

Thus, the corollary can be rephrased to say:

Corollary 7.6. *The category of R-modules is an additive category.*

7.3. **projective modules.**

Definition 7.7. A module M is called *projective* if, for any epimorphism $p : A \to B$ and any morphism $f : M \to B$, there is a morphism $\tilde{f} : M \to A$ so that $p \circ \tilde{f} = f$. I.e., the following diagram commutes.



(1) Free modules are projective.
(2) What happens when B is projective?
(3) Partial converse for (1).
(4) Example.

7.3.1. *free ⇒ projective.*

Theorem 7.8. *Free modules are projective.*

Proof. Suppose that $M = F(X)$ is the free R-module on the set X. We have a homomorphism $f : F = M \to B$ and we want to lift it to a homomorphism $\tilde{f} : F \to A$.

We need the following adjunction property.

$$\mathrm{Hom}_R(F(X), A) \cong \mathrm{Hom}_{\mathcal{E}ns}(X, A)$$

Any homomorphism $F(X) \to A$ gives a set map $X \to A$ by restriction and any set map $g : X \to A$ extends uniquely to a homomorphism $g' : F(X) \to A$ by the formula

$$g'\left(\sum r_i x_i\right) = \sum r_i g(x_i).$$

In this case, $g : X \to A$ is given by the fact that p is surjective: For any $x_i \in X$, $f(x_i) = b_i \in B$ comes from some element $a_i \in A$. Let $g(x_i) = a_i$. Then the lifting $\tilde{f} : F \to A$ is given by

$$\tilde{f}\left(\sum r_i x_i\right) = \sum r_i g(x_i) = \sum r_i a_i.$$

This is a lifting of f since

$$f\left(\sum r_i x_i\right) = \sum r_i f(x_i) = \sum r_i b_i = p\left(\sum r_i a_i\right) = p\tilde{f}\left(\sum r_i x_i\right)$$

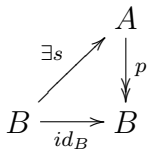
□

7.3.2. *What if B were projective?*

Theorem 7.9. *If $p : A \to B$ is onto and B is projective then*

$$A \cong B \oplus \ker p.$$

Proof. What students immediately realized is that there is a mapping $s : B \to A$. This follows from the definition of a projective module applied to the following diagram.



The morphism $s : B \to A$ is called a *section* of p because it satisfies the condition $p \circ s = id_B$. So, we have a morphism $s : B \to A$ and we also have the inclusion map $j : \ker p \to A$. Together they give a morphism

$$s \oplus j : B \oplus \ker p \to A.$$

This is the homomorphism given on elements by

$$(b, x) \mapsto s(b) + x.$$

We need to show that this is 1-1 and onto.

To show that it is onto, take any $a \in A$. Then a clearly comes from the element

$$(p(a), a - sp(a)) \in B \oplus \ker p.$$

We just have to show that $a - sp(a)$ actually lies in $\ker p$. This is a calculation:

$$p(a - sp(a)) = p(a) - pap(a) = p(a) - (id)p(a) = p(a) - p(a) = 0.$$

To show that the mapping is 1-1, suppose that $(b, x), (b', x')$ map to the same element of A. Then

$$s(b) + x = s(b') + x' \Rightarrow$$

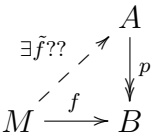
$$p(s(b) + x) = ps(b) = b = p(s(b') + x') = ps(b') = b'$$

And this implies $s(b) = s(b')$. So, $x = x'$. So, the map is a bijection. □

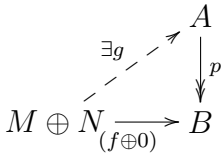
7.3.3. *partial converse.* The partial converse to the first statement is the following.

Theorem 7.10. *A module M is projective if and only if it is a direct summand of a free module.*

Proof. We know that free modules are projective. We can conclude from this that direct summands of free modules are projective. Suppose we have the diagram:



Suppose that $M \oplus N = F$ is free. Then, we get another diagram:



The lifting g exists since $M \oplus N$ is projective. But then $\tilde{f} = g|M$ is a solution of the original lifting problem. So, M is projective.

Conversely, suppose that M is projective. Then, we know that there is an epimorphism

$$p : F \to M$$

where F is free. But we just showed that, under these conditions, $F \cong M \oplus \ker p$. So, M is a direct summand of the free module F. □

7.3.4. *example.* Here is a simple example of a projective module which is not free. Let $R = M_n(K)$ be the ring of $n \times n$ matrices with coefficients in K. Then $F = R$ is a free module with action of R given by left multiplication, i.e., row operations. Matrix multiplication has the property that the entries in the different columns do not mix. (You need column operations, given by right multiplication by matrices, to do that.) Therefore, the n column vectors are direct summands. More precisely, let C_j be the set of all matrices whose entries are zero except possibly in column j. Then, we have the direct sum decomposition:

$$F = C_1 \oplus C_2 \oplus \cdots \oplus C_n$$

So, each C_j is projective (being a direct summand of the free module F). But C_j is not free since it is only n-dimensional over K and the dimension of every free module is a multiple of n^2. Note that the C_j are all isomorphic.

7.4. **finite generation.** We know that finite sums are the same as finite products. When the index set I is infinite (and the modules M_α are all nonzero), the definitions are certainly different:

$$\bigoplus M_\alpha \neq \prod M_\alpha.$$

But there is more. These are not just computationally distinct. They are conceptually different. For example, an infinite direct sum cannot be finitely generated but an infinite product can.

Theorem 7.11. *An infinite direct sum of nonzero modules cannot be finitely generated.*

Proof. Suppose that $\bigoplus M_\alpha$ has a finite set of generators $x_1, \cdots, x_n$. Then each x_i has only finitely many nonzero coordinates. Let $\beta \in I$ be a coordinate which is not one of these. Then any linear combination $\sum r_i x_i$ will also have zero as its β coordinate. So, we don't get the entire sum $\bigoplus M_\alpha$. □

Theorem 7.12. *It is possible for an infinite product of nonzero modules to be finitely generated.*

Proof. Let $R = \prod R_\alpha$ be an infinite product of rings. This is a ring. In particular it has unity: $1 = (1, 1, \cdots)$. Let $F = R$ be the free module with one generator (1). Let $M_\alpha = R_\alpha$. This is an R-module for each α. The product is

$$\prod M_\alpha = \prod R_\alpha = F$$

which is finitely generated. □

Challenge: Can you find an example where R is a reasonable ring?

8. Finite generation and ACC

I continued the discussion of finitely generated modules by talking about Noetherian modules and rings. One example lead to a discussion of the "restriction of scalars" functor and the basis theorem for finite dimensional vector spaces over a field. This is a precursor to the fundamental theorem for f.g. modules over a PID and applications to matrices.

8.1. **Noetherian rings and modules.**

8.1.1. *definitions.*

Definition 8.1. If M is an R-module, an An *ascending chain* of submodules of M is an increasing sequence of submodules:

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq M$$

We say that M satisfies the *ascending chain condition* (ACC) for submodules if every such sequence stops, i.e., if there is a k so that $N_n = N_k$ for all $n \geq k$.

Definition 8.2. A module M is *Noetherian* if it satisfies the ACC for submodules. A commutative ring R is called *Noetherian* if it satisfies the ACC for ideals. This is equivalent to saying that R is a Noetherian when considered as an R-module. (A noncommutative ring is called *left-Noetherian* if it satisfies the ACC for left ideals.)

8.1.2. *examples.* The first example I gave was $\mathbb{Z}$.

Theorem 8.3. *$\mathbb{Z}$ is Noetherian (as a ring and as a module over $\mathbb{Z}$).*

I proved this twice. The first time, I used the properties of the integers. The second time I used only the fact that $\mathbb{Z}$ is a PID.

Proof. To show that $\mathbb{Z}$ is Noetherian we took an ascending chain:

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq \mathbb{Z}$$

Each submodule N_i is an ideal (or $\mathbb{Z}$) generated by one element $n_i \geq 0$ and the condition $N_i \subseteq N_{i+1}$ is equivalent to saying that n_{i+1} divides n_i. In particular, $n_{i+1} \leq n_i$. So,

$$n_1 \geq n_2 \geq n_3 \geq \cdots .$$

Since these numbers are bounded below (by 0), the sequence stops (becomes constant) at some point. Thus $n_k = n_{k+1} = \cdots$. This is equivalent to saying that

$$N_k = N_{k+1} = \cdots .$$

So, the ACC holds and $\mathbb{Z}$ is Noetherian. □

Second proof. In the second proof, I took the union of the N_i and called it N_∞

$$N_\infty = \bigcup_{i=1}^{\infty} N_i.$$

This is a submodule of $\mathbb{Z}$ since it is closed under addition and scalar multiplication: If $a \in N_i$ and $b \in N_j$ where $i \leq j$ then $a + b \in N_j$. The submodule N_∞ is generated by one element n_∞ which is contained in some N_k. But then:

$$(n_\infty) \subseteq N_k \subseteq N_{k+1} \leq N_{k+2} \leq \cdots \subseteq N_\infty = (n_\infty).$$

So,

$$N_k = N_{k+1} = N_{k+2} = \cdots$$

as before. □

The second proof works for any PID. This is Corollary 8.6 below.

Some other easy examples of Noetherian rings and modules are the following.

(1) Any finite ring or module is Noetherian.
(2) Any quotient of a Noetherian ring or module is Noetherian.
(3) A finite product of Noetherian rings is Noetherian. (Proof: Every ideal in $R \times S$ has the form $I \times J$ where I is an ideal in R and J is an ideal in S. In any ascending chain $(I_n \times J_n)$, both sequences I_n and J_n have to stop.)

8.1.3. *theorem.* Here is the general theorem about Noetherian modules.

Theorem 8.4. *An R-module is Noetherian M if and only if every submodule is finitely generated.*

Corollary 8.5. *A commutative ring is Noetherian if and only if every ideal is finitely generated.*

Corollary 8.6. *Every PID is Noetherian.*

Proof. Suppose first that M has a submodule N which is not finitely generated. Then, any finite subset of N will generate a proper submodule.

Let $x_1 \in N$. Then $Rx_1 \subsetneq N$. So, there is an $x_2 \in N$, $x_2 \notin Rx_1$. Then $Rx_1 + Rx_2 \subsetneq N$. So, there is an $x_3 \in N \backslash Rx_1 + Rx_2$. Continuing in this way, we get a strictly increasing sequence of submodules

$$Rx_1 \subsetneq Rx_1 + Rx_2 \subsetneq Rx_1 + Rx_2 + Rx_3 \subsetneq \cdots$$

So, the ACC fails and M is not Noetherian.

Conversely, suppose that every submodule of M is finitely generated. Then we have to show that any ascending chain:

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq M$$

stops. To show this take the union

$$N_\infty = \bigcup N_i$$

This is a submodule of M and is therefore finitely generated. Let $x_1, \cdots, x_n$ be the generators. Then each x_i is contained in some N_j. If k is the maximum of the indices j then all the x_i will be contained in N_k. But then N_k must equal N_∞. So,

$$N_k = N_{k+1} = N_{k+2} = \cdots$$

and the ACC holds. So, M is Noetherian. □

8.2. **restriction of scalars.** I explained one example of a Noetherian module which used restriction of scalars and the basis theorem for f.g. vector spaces. I explained these tools after the example. So, I will do the same thing here.

Example 8.7. Let R be the polynomial ring $R = F[T]$ over a field F. Then a module M can be constructed as follows. Suppose that A is an $n \times n$ matrix with coefficients in the field F. Then $M = F^n$ is a module if we define the action of a polynomial $p(T) = \sum r_i T^i \in R = F[T]$ by

$$p(T)x = \sum r_i A^i x$$

then M is a Noetherian R-module. To see this take any ascending chain of submodules:

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq M$$

Since R contains the ground field F, every R-module is also a vector space over F. Thus every N_i is a vector space over F. So, it has a dimension d_i. Since $M \cong F^n$, its dimension is n. So,

$$d_1 \leq d_2 \leq d_3 \leq \cdots \leq n$$

This implies that the sequence stops, i.e., there is a $k \geq 1$ so that

$$d_k = d_{k+1} = \cdots$$

But, every proper subspace of a vector space has smaller dimension, so

$$N_k = N_{k+1} = \cdots$$

I.e., the ACC holds and M is Noetherian.

The key point is the realization that an R-module is also a vector space over F. This is called "restriction of scalars." The definition is as follows.

Definition 8.8. Suppose that either

(1) S is a subring of R or
(2) $\phi : S \to R$ is a ring homomorphism. (We can let $\phi : S \to R$ be the inclusion map to make (1) a special case of (2).)

Then, in either case, we get a *restriction of scalars* functor

$$\phi^* : R\text{-Mod} \to S\text{-Mod}$$

given on objects by $\phi^*(M) = M$ considered as an S-module in the following way:

(1) When $S \subseteq R$ we just restrict the action of R. So, for any $a \in S$ and $x \in M$ we let $ax = ax$. This makes sense since $a \in R$.
(2) In the general case we let $sx = \phi(s)x$. In other words, the action of S on M is given by the composition

$$S \xrightarrow{\phi} R \xrightarrow{\alpha} \mathrm{End}_{\mathbb{Z}}(M)$$

where α is the action of R on M.

Just as $\phi^*(M) = M$ with a different action, $\phi^*(f : M \to N)$ is also the same mapping $f : M \to N$ considered as a homomorphism of S-modules.

The other fact that we used in the last example was our knowledge of linear algebra over any field. I decided to go over some of that.

8.3. **finite dimensional vector spaces.** Recall that a module over a field F is the same as a vector space. So I called it V. Suppose V is finitely generated with generators $v_1, v_2, \cdots, v_n$. In linear algebra we say that these vectors *span* V and every element of V is a linear combination of these vectors:

$$(\forall x \in V)(\exists x_1, \cdots, x_n \in F) \quad x = x_1v_1 + x_2v_2 + \cdots + x_nv_n$$

This is equivalent to saying that we have an epimorphism

$$\phi : F^n \to V$$

$$(x_1, \cdots, x_n) \mapsto \sum x_iv_i$$

The set $\{v_1, \cdots, v_n\}$ is a *basis* for V if this mapping is an isomorphism.

8.3.1. *existence of a basis.*

Lemma 8.9. *If the epimorphism $\phi : F^n \to V$ is not an isomorphism then V is generated by $n-1$ elements.*

This lemma implies the existence of a basis for a finitely generated vector space. (The word "dimension" is not yet justified. Since this is defined to be the number of elements in a basis, we need to show that this number is unique to show that dimension is well-defined.)

Theorem 8.10. *Any minimal finite spanning set for a vector space V is a basis.*

As I pointed out the next day, this implies the following.

Corollary 8.11. *Every finite spanning set for a vector space contains a basis.*

Proof of Lemma. Suppose that $\phi : F^n \to V$ is not an isomorphism. Then $\ker \phi \neq 0$. So, there is a nonzero element $x \in \ker \phi$. But $x = (x_1, \cdots, x_n)$ being nonzero means one of the coordinates is nonzero. Say $x_1 \neq 0$. Then $x_1^{-1} \in F$. So,

$$v_1 = \sum_{i=2}^{n} \frac{x_i v_i}{x_1}$$

which means that the $n-1$ vectors $v_2, \cdots, v_n$ span V as claimed. □

8.3.2. *dimension.* On the next day, I showed that the number of elements in a finite basis is uniquely determined.

Theorem 8.12. *If V is a finitely generated vector space over a field F then any two bases for V have the same number of elements.*

Proof. By Theorem 8.10, V has a finite basis. The proof will be by induction on n, the size of the smallest basis for V.

Suppose the theorem were not true. Then $F^n \cong V \cong F^m$ where $m > n$. Let $v_1, \cdots, v_m \in V$ be a basis with the larger number of elements. Let $W = Fv_m$. Then $V/W \cong F^{m-1}$ since $v_1 + W, \cdots, v_{m-1} + W$ form a basis. The homomorphism

$$\phi : F^n \cong V \twoheadrightarrow V/W$$

is onto with nontrivial kernel $\ker \phi = W$. So, by Lemma 8.9, V/W is generated by $n-1$ elements. By Corollary 8.11, this implies that V/W has a basis with $\leq n-1$ elements. By induction on n, all bases for V/W have the same size. This is a contradiction since we know that V/W has a basis with $m-1$ elements. □

9. Modules over a PID

This week we are proving the fundamental theorem for finitely generated modules over a PID, namely that they are all direct sums of cyclic modules. The proof will be in stages. On the first day I decomposed a module into a torsion and torsion-free part. The presentation was a little disorganized so that the steps do not follow one after the other but rather the other way around, i.e., to prove (1) we need to prove (2) and to prove (2) we need to prove (3), etc. I call this the "motivational order." At the end we will go over the lemmas and put them in correct logical order.

9.1. **torsion and torsion-free.** Suppose that R is a PID and M is a finitely generated R-module. The main example I talked about was $R = \mathbb{Z}$ in which case $M = G$ is a f.g. abelian group.

Definition 9.1. M is *torsion-free* if $ann(x) = 0$ for all $x \neq 0$ in M.

Definition 9.2. M is *torsion* if $ann(x) \neq 0$ for all $x \neq 0$ in M.

For example, R itself is torsion-free and $R/(a)$ is torsion. In the case $R = \mathbb{Z}$, $\mathbb{Z}^n$ and $\mathbb{Q}$ are torsion-free additive groups. However, $\mathbb{Q}$ is not finitely generated. The finitely generated torsion abelian groups are exactly the finite abelian groups.

The first decomposition theorem is the following.

Theorem 9.3. *Every f.g. module over a PID is a direct summand of a torsion module and a torsion-free module:*

$$M \cong tM \oplus fM$$

where tM is torsion and fM is torsion free.

The second theorem tells us what the torsion-free part looks like:

Theorem 9.4. *A f.g. module over a PID is torsion-free if and only if it is free:*

$$fM \cong R^n.$$

9.1.1. *torsion submodule.* I used two lemmas to show that the second theorem implies the first theorem. During the class we decided that these two lemmas hold over any domain. First I need a definition.

Definition 9.5. Suppose that M is a module over a domain R. Then the *torsion submodule* of M is defined to be the set of all elements of M with nonzero annihilator ideal:

$$tM := \{x \in M \mid ann(x) \neq 0\}$$

Lemma 9.6. *tM is a submodule of M provided that R is a domain.*

Proof. We need to show that tM contains 0 and is closed under addition and scalar multiplication.

(1) $0 \in tM$ since $ann(0) = R$.
(2) If $x, y \in tM$ then there are nonzero elements $a, b \in R$ so that $ax = by = 0$. Then $ab(x + y) = 0$. So, $x + y \in tM$.
(3) If $x \in tM$ and $r \in R$ then $ann(rx) \supseteq ann(x)$ is nonzero.

In the second step we need to know that $ab \neq 0$. □

Lemma 9.7. *The quotient M/tM is torsion-free provided that R is a domain.*

Proof. Suppose not. Then there is a nonzero element $x + tM$ in M/tM and $a \neq 0$ in R so that $ax + tM$ is zero, i.e., $ax \in tM$. But this means there is a nonzero element $b \in R$ so that $bax = 0$. But $ba \neq 0$. So, $x \in tM$ which is a contradiction. □

It was in this proof that I mentioned the *fraction notation*:

$$(tM : x) := \{a \in R \,|\, ax \in tM\}.$$

Next, I showed that the second theorem (Theorem 9.4) implies the first (Theorem 9.3).

Proof of Theorem 9.4. Let $fM = M/tM$. Since this is free, there is a section $s : fM \to M$ of the projection map $M \to M/tM$. Then

$$j \oplus s : tM \oplus fM \to M$$

is an isomorphism where $j : tM \to M$ is the inclusion map. □

Next, we need to prove that f.g. torsion-free modules are free and that f.g. torsion modules are direct sums of cyclic modules. I intend to use "purity" to do both.

9.1.2. *pure submodules.*

Definition 9.8. We say that a submodule $N \subseteq M$ is *pure* if whenever $x \in M$ and $a \in R$ with $ax \in N$ there exists $z \in N$ so that $az = ax$. In other words: "If an element of N is divisible by $a \in R$ in M then it is divisible by a in N."

The point is that pure submodules are direct summands in f.g. modules over PID's. However, using this fact is a little tricky as we saw the next day.

On the second day I pointed out that if P is a pure submodule of a f.g. module M over a PID, then P is a direct summand. However, we cannot use this fact to prove the main theorem because it uses the main theorem, namely that f.g. modules are direct sums of cyclic modules. However, we use the main theorem on a module with a fewer number of generators than M. So, this can be used in an inductive proof of the main theorem. The theorem is:

Theorem 9.9. *Suppose that P is a pure submodule of a f.g. module M over a PID R and M/P is a direct sum of cyclic modules. Then P is a direct summand of M.*

Proof. Suppose that M/P is a direct summand of cyclic modules. Then each summand is generated by some element $x_i + P$ with annihilator (a_i). This means that $(x_i : P) = (a_i)$. In other words, $a_i x_i \in P$. Since P is pure, there is an element $z_i \in P$ so that $a_i z_i = a_i x_i$. But then

$$x_i + P = (x_i - z_i) + P$$

and $a_i(x_i - z_i) = 0$. So $s_i(x_i + P) = x_i - z_i$ gives a lifting $s_i : R/(a_i) \to M$ of the direct summand $R/(a_i)$ of M/P to M and, together, these give an isomorphism

$$\left(\bigoplus s_i\right) \oplus j : \bigoplus R/(a_i) \oplus P \xrightarrow{\approx} M$$

where $j : P \to M$ is the inclusion map. □

To find the pure submodule, I need to take a maximal cyclic submodule of M. This exists because M is Noetherian. So that is next.

9.2. **submodules of free modules.**

Theorem 9.10. *Suppose that $M = R^n$ is a free R-module with n generators where R is a PID. Then any submodule of M is free with n or fewer generators.*

Proof. This is by induction on n. If $n = 1$ then $M = R$ and the submodules are either R or an ideal Rx. But R is a domain. So, either $x = 0$ or $ann(x) = 0$. So, Rx is free with 0 or 1 generator.

Now suppose that $n \geq 2$ and N is a submodule of R^n. Then we want to show that $N \cong R^m$ where $m \leq n$. Let $e_1, \cdots, e_n$ be the free generators of $M = R^n$. Let R^{n-1} denote the free submodule of M generated by $e_1, \cdots, e_{n-1}$. Then, by induction on n, we have:

$$N \cap R^{n-1} \cong R^{m-1}$$

where $m \leq n$. If $N = N \cap R^{n-1}$ we are done. Otherwise, let J be the set of all e_n coordinates of all elements of N. I.e.,

$$J = \left\{ a \in R \,|\, (\exists x \in N)\ x = ae_n + \sum_{i=1}^{n-1} a_i e_i \right\}$$

We get at least one nonzero element in J since N is not contained in R^{n-1}. Then it is easy to see that J is an ideal (or all of R) since it is closed under addition and scalar multiplication and is nonempty. Therefore, $J = (b)$ is generated by one element $b \neq 0$. (So, every $a \in J$ has the form $a = rb$ where $r \in R$ is unique.)

By definition, there is an element $x_0 \in N$ so that

$$x_0 = be_n + \sum_{i=1}^{n-1} a_i e_i.$$

This can be used to define a homomorphism

$$\phi : (N \cap R^{n-1}) \oplus R \to N$$

by $\phi(y, r) = y + rx_0$. I claim that ϕ is an isomorphism.

To see that ϕ is onto, take any element $x \in N$. Then $x = ae_n +$ (some element of R^{n-1}) where $a = rb$. So,

$$x - rx_0 \in N \cap R^{n-1}$$

and $x = \phi(x - rx_0, r)$. To see that ϕ is 1-1 suppose that $\phi(y, r) = 0$. Then $y = -rx_0$. Looking at the last coordinate this gives $rb = 0 \Rightarrow r = 0 \Rightarrow y = 0$. Therefore ϕ is an isomorphism. Its inverse gives:

$$N \cong (N \cap R^{n-1}) \oplus R \cong R^{m-1} \oplus R \cong R^m$$

where $m \leq n$. □

Corollary 9.11. *If M is an R-module generated by n elements then every submodule of M is generated by $\leq n$ elements. In particular, M is Noetherian.*

Proof. If M is generated by $x_1, \cdots, x_n$ then we have an epimorphism

$$\phi : R^n \twoheadrightarrow M$$

given by $\phi(a_1, \cdots, a_n) = \sum a_i x_i$. If $N \subseteq M$ then N is a quotient of $\phi^{-1}N$ which is free on $\leq n$ generators by the theorem. □

9.3. **maximal cyclic submodules.** Since f.g. modules are Noetherian, they have maximal cyclic submodules. This is because any sequence of cyclic submodules:

$$Rx_1 \subseteq Rx_2 \subseteq Rx_3 \subseteq \cdots \subseteq M$$

must eventually stop. (If there were no maximal cyclic submodule, I could keep going forever.)

Lemma 9.12. *Suppose that M is torsion-free and $Rx \subseteq M$ is a maximal cyclic submodule. Then $x \notin aM$ for any nonunit $a \in R$. (I.e., $x = az \Rightarrow a$ is a unit.)*

Proof. Suppose that $x = az$. Then $Rx \subseteq Rz$. Since Rx is maximal cyclic, $Rx = Rz$ which implies that $z = bx$ for some $b \in R$. So, $x = az = abx$ which implies $(ab - 1)x = 0$. Since M is torsion-free, this implies that $ab = 1$, i.e., a is a unit. □

Lemma 9.13. *Every maximal cyclic submodule of a torsion-free module is pure.*

Proof. Suppose that $Rx \subseteq M$ is a maximal cyclic submodule. Suppose there are elements $y \in M, a \in R$ so that $ay \in Rx$. Then $ay = bx$. We need to show that this is a times an element of Rx. In other words, we want to show that $a|b$ (a divides b). This is the same as saying that $\frac{b}{a} \in R$.

At this point I explained this equivalent formulation of divisibility. Since R is a domain, it is contained in its field of fractions: $R \subseteq Q(R)$. The fraction $\frac{b}{a}$ is an element of $Q(R)$. If $a|b$, then $b = ra$ for some $r \in R$ and

$$\frac{b}{a} = \frac{r}{1} \in R$$

and conversely. So, $a|b \Leftrightarrow \frac{b}{a} \in R$.

Let $c \in R$ be the greatest common divisor of a, b. I.e., $(a, b) = (c)$. Then $c|a$ and $c|b$. I.e., $\frac{a}{c}, \frac{b}{c} \in R$ and

$$\frac{a}{c}\, y = \frac{b}{c}\, x$$

since M is torsion-free. (c times the difference is zero. So, the difference is zero.) But $(\frac{a}{c}, \frac{b}{c}) = (1)$, i.e., there exist $s, t \in R$ so that

$$1 = \frac{a}{c}\, s + \frac{b}{c}\, t.$$

This implies that

$$x = \frac{a}{c}\, sx + \frac{b}{c}\, tx = \frac{a}{c}\, sx + \frac{a}{c}\, ty = \frac{a}{c}(sx + ty)$$

since $bx = ay$. By the previous lemma, this implies that $\frac{a}{c}$ is a unit, i.e., $\frac{c}{a} \in R$. So

$$\frac{b}{a} = \frac{b}{c}\frac{c}{a} \in R$$

as desired. □

We need one more lemma.

Lemma 9.14. *If P is a pure submodule of a torsion-free module M then M/P is torsion-free.*

Proof. Suppose not. Then there is a nonzero element $x + P \in M/P$ so that $a(x + P) = 0 + P$. I.e., $ax \in P$. But P is pure. So, there is $z \in P$ so that $az = ax$. Then $a(x - z) = 0$ in M which implies that $x = z$ since M is torsion free. So, $x + P = z + P = P$ is the zero element of M/P which is a contradiction. □

Now I am ready to prove Theorem 9.4: Finitely generated torsion-free modules over PID's are free, completing the proof that

$$M \cong tM \oplus fM \cong tM \oplus R^n.$$

Proof of Theorem 9.4. The proof is by induction on the number of generators. If M has one generator x then $M = Rx \cong R$ is free. So, suppose M has n generators $x_1, \cdots, x_n$ where $n \geq 2$. Since Rx_1 is a cyclic submodule of M it is contained in a maximal cyclic submodule Rx. By Lemma 9.13, Rx is pure. By Lemma 9.14, this implies that M/Rx is torsion-free. But M/Rx is generated by $n - 1$ elements (the images of the generators $x_2, \cdots, x_n$). So, it is free, say, $M/Rx \cong R^m$. But this implies that

$$M \cong Rx \oplus R^m \cong R \oplus R^m$$

is also free. □

It remains to show that the torsion submodule tM is also a direct sum of cyclic modules. I want to do the same proof, namely, since M is Noetherian, we can find a maximal cyclic submodule Rx. Since M/Rx will be generated by $n - 1$ elements, it is a sum of cyclic modules.

After some stumbling, I decided I need a more precise construction of a maximal cyclic submodule. I took a generator with minimal annihilator. And this works the best for p-primary modules.

9.4. **p-primary decomposition.** p-primary modules are generalizations of abelian p-groups. We showed that finite nilpotent groups are products of their p-Sylow subgroups. For finite abelian groups and, more generally, for torsion modules over PID's, this is very easy to prove. It follows from the unique factorization theorem. (I.e., every PID is a UFD.)

Definition 9.15. An element $x \in M$ is called *p-primary* if it has annihilator

$$ann(x) = (p^n)$$

for some $n \geq 0$ where $p \in R$ is irreducible. A module M is called *p-primary* if every element is p-primary. (Note that $0 \in M$ is p-primary for every p.)

I should have prove the following lemma first:

Lemma 9.16. *If $p^n x = 0$ where $n \geq 0$ then x is p-primary.*

Proof. Suppose $ann(x) = (a)$. Then $p^n x = 0$ implies that $p^n = ab$ for some $b \in R$. By unique factorization this implies that $a = up^k$ where u is a unit in R and $k \leq n$. But then $ann(x) = (up^k) = (p^k)$. □

For modules over a PID, the "Sylow theorems" are very easy to prove:

Lemma 9.17. *The set of p-primary elements of any module M over a PID is a submodule.*

Definition 9.18. If $p \in R$ is irreducible, let M_p be the submodule of M consisting of all p-primary elements of M.

Proof. If x, y are nonzero p-primary elements of M then $p^n x = 0$ and $p^m y = 0$. Then $p^n rx = 0$ for any $r \in R$ and $p^{n+m}(x+y) = 0$. Therefore, rx and $x + y$ are p-primary by the lemma. □

Theorem 9.19. *Every torsion module M over a PID is a direct sum of p-primary modules:*

$$M = \bigoplus_p M_p.$$

Proof. First choose irreducible elements p_i so that every irreducible element of R is up_i for some unit u and some unique p_i. By the lemma, for each of these irreducibles we have a submodule $M_{p_i} \subseteq M$. By the universal property this gives a homomorphism

$$\phi : \bigoplus M_{p_i} \to M$$

I claim that this is an isomorphism.

It follows from unique factorization that this map is onto: Suppose $x \neq 0 \in M$ with annihilator $ann(x) = (a)$. Since M is torsion, $a \neq 0$. So

$$a = u \prod_{i=1}^{k} p_i^{n_i}$$

where u is a unit. Then, for each i,

$$\frac{a}{p_i^{n_i}} = u p_1^{n_1} \cdots \widehat{p_i^{n_i}} \cdots p_k^{n_k} \in R.$$

There is no irreducible element of R which divides each of these elements. This implies that there are elements $r_i \in R$ so that

$$1 = \sum_{i=1}^{k} r_i \frac{a}{p_i^{n_i}}.$$

Apply this to x to get:

$$x = \sum_{i=1}^{k} r_i \frac{a}{p_i^{n_i}} x = \sum_{i=1}^{k} r_i x_i$$

where

$$x_i = \frac{a}{p_i^{n_i}} x$$

is p_i-primary since $p_i^{n_i} x_i = ax = 0$. This shows that $x = \phi(r_i x_i)_i$ is in the image of ϕ and therefore ϕ is onto.

To show that ϕ is 1-1 suppose that $(x_i)_i$ is in the kernel of ϕ. Then

$$\sum_{i=1}^{k} x_i = 0$$

where x_i is p_i-primary. Thus sum is finite since the direct sum is equal to the weak product. Suppose that $ann(x_i) = (p_i^{n_i})$. Then the product $p_2^{n_2} \cdots p_k^{n_k}$ annihilates $x_2, \cdots, x_k$ and therefore annihilates their sum

$$x_2 + \cdots + x_k = -x_1$$

This implies that $p_2^{n_2} \cdots p_k^{n_k} \in (p_1^{n_1})$, i.e.,

$$p_2^{n_2} \cdots p_k^{n_k} = a p_1^{n_1}$$

for some $a \in R$. By unique factorization this is only possible if $n_1 = 0$, i.e., $x_1 = 0$. The same argument shows that $x_i = 0$ for all i. So, ϕ is a monomorphism and thus an isomorphism as claimed. $\square$

9.5. **decomposition of p-primary modules.** Now we come to the final step in the proof of the main theorem, namely, I will prove that every f.g. p-primary module is a direct sum of cyclic modules. But first some lemmas.

Lemma 9.20. *Any quotient of a p-primary module is p-primary.*

Proof. This is obvious. If $x \in M$ then $p^n x = 0$ for some n. But then $p^n(x + N) = 0$ in M/N. So, M/N is p-primary. □

Lemma 9.21. *Suppose M is a f.g. p-primary module and $a \in R$ so that $p \not| a$. Then, there is a $b \in R$ so that multiplication by ab is the identity on M.*

Proof. Let $x_1, \cdots, x_k$ be generators for M and suppose that $ann(x_i) = p^{n_i}$. Let $n = \max(n_i)$. Then $p^n M = 0$. Since $a \notin (p)$, $(a, p^n) = (1)$. So, there exist $b, c \in R$ so that

$$ab + p^n c = 1$$

But $p^n = 0$ on M. So, $ab = 1$ on M. □

Theorem 9.22. *If M is a f.g. p-primary module over a PID R then M is a direct sum of cyclic p-primary modules.*

Proof. Let $x_1, \cdots, x_k$ be generators for M where k is minimal. Then we will show by induction on k that M is a direct sum of k or fewer cyclic summands. Since M/Rx_1 is generated by $k - 1$ elements, it is a direct sum of $\leq k - 1$cyclic p-primary modules by induction. So, it suffices to show that Rx_1 is a pure submodule of M.

Let $ann(x_i) = p^{n_i}$ and let $n = \max(n_i)$. We will assume that $n = n_1$. Then $p^n M = 0$ and

$$p^{n-1} x_1 \neq 0.$$

Claim Rx_1 is a pure submodule of M.

proof: Suppose that $y \in M$ and $a \in R$ so that $ay \in Rx_1$. If $ay = 0$ then $ay = a0 \in aRx_1$. So, we may assume that $ay \neq 0$. Then $ay = bx_1$ for some $b \in R$. Write a, b as $a = p^k s, b = p^m t$ where s, t are not divisible by p. The condition $ay = p^m t x_1 \neq 0$ means that $m < n$. So,

$$n - m - 1 \geq 0.$$

By the lemma, there is an element $r \in R$ so that $sr = 1$ on M. This gives:

$$ay = p^k sy = p^m t x_1 = p^m srt x_1 \tag{9.1}$$

So, it suffices to show that $k \leq m$ since this would give $ay = a(p^{m-k} rt x_1)$. To prove that $k \leq m$ multiply both sides of Equation (9.1) by p^{n-m-1}.

This gives

$$p^{k+(n-m-1)}sy = p^{m+(n-m-1)}tx_1 = p^{n-1}tx_1 \neq 0$$

since $p^{n-1}x_1 \neq 0$ and multiplication by t is an isomorphism on M. But this implies that the left hand side is also nonzero. Since $p^n M = 0$ this implies that

$$k + n - m - 1 < n$$

In other words, $k < m + 1$ or $k \leq m$. This proves the claim and the theorem. $\square$

9.6. **Structure theorem for f.g. modules over a PID.** Now we have the complete proof of the following existence theorem.

Theorem 9.23. *Every f.g. module over a PID is a direct sum of cyclic primary modules*

$$M \cong R^r \oplus \bigoplus R/(p_i^{n_i}).$$

Proof. Here is an outline of the entire proof.

(1) First, we defined the torsion submodule tM of M. This exists since R is a domain.
(2) The quotient M/tM is torsion-free. Again this holds over any domain.
(3) Since R is a PID, every submodule of a f.g. free module is f.g. free. This implies:
   (a) M is Noetherian (all submodules are finitely generated) and
   (b) Every f.g. torsion-free module is free.
(4) The conclusion was that M is a direct sum of tM and a f.g. free module:
$$M \cong tM \oplus R^r$$
(5) If $p \in R$ is irreducible, the set of p-primary elements of any module forms a submodule M_p.
(6) It follows from unique factorization that every torsion module is a direct sum of p-primary modules:
$$tM \cong \bigoplus M_{p_i}$$
(7) In a p-primary module M, a generator with minimal annihilator generates a pure cyclic submodule. Then we use the lemma:
(8) If N is a pure submodule of M and M/N is a direct sum of cyclic modules then N is a direct summand of M.
(9) Every f.g. p-primary module is a direct sum of cyclic p-primary modules.

□

The structure theorem for finitely generated modules over a PID also says the decomposition is unique:

Theorem 9.24. *For any f.g. module M over a PID, the numbers r and the sequence of pairs (p_i, n_i) are uniquely determined up to permutation of indices.*

We will prove this later using tensor products. The number $r = rk(M)$ is called the *rank* of M. It is the dimension of $Q(R) \otimes M$.

10. Jordan canonical form

As an application of the structure theorem for PID's I explained the *Jordan canonical form* for matrices over the complex numbers. First I stated the theorem and then I proved it by reducing it to a module over a PID.

10.1. **statement of the theorem.** The theorem is that any $n \times n$ matrix A with coefficients in the complex numbers is conjugate to a matrix in Jordan canonical form. This is defined to be a square matrix with the eigenvalues of A along the diagonal, 0's and 1's on the super-diagonal (right above the diagonal) and zeroes everywhere else. Also, if there is a 1 in the $i, i+1$ position then $a_{ii} = a_{i+1,i+1}$. Here is an example:

$$B^{-1}AB = \begin{pmatrix} a & 1 & 0 & 0 & 0 & 0 \\ 0 & a & 1 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & b & 1 \\ 0 & 0 & 0 & 0 & 0 & b \end{pmatrix}.$$

This is a matrix with three *Jordan blocks*

$$B^{-1}AB = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix} \oplus (a) \oplus \begin{pmatrix} b & 1 \\ 0 & b \end{pmatrix}.$$

On the second day, I used the notation $[\lambda]^k$ to denote the Jordan block of size k and eigenvalue λ. So, this decomposition would be written:

$$B^{-1}AB = [a]^3 \oplus [a]^1 \oplus [b]^2.$$

10.2. **module over a PID.** The key point is something I explained earlier. Namely, any square matrix over $\mathbb{C}$ makes $\mathbb{C}^n$ into a module over $\mathbb{C}[T]$.

If A is an $n \times n$ matrix over $\mathbb{C}$ then A is an element of the matrix ring $M_n(\mathbb{C})$. We let $R = \mathbb{C}[T]$. This is a PID since $\mathbb{C}[T]$ has a Euclidean algorithm: when you divide one polynomial by another, the remainder has smaller degree. The module is $M = \mathbb{C}^n$ with the action of the ring given by the evaluation map

$$ev_A : \mathbb{C}[T] \to M_n(\mathbb{C})$$

which sends $f(T)$ to $f(A)$. In other words,

$$f(T)x = f(A)x.$$

For example, if $f(T) = aT^2 + bT + c$ then

$$f(T)x = f(A)x = aA^2x + bAx + cx.$$

Lemma 10.1. *$M = \mathbb{C}^n$ is a finitely generated torsion module over $R = \mathbb{C}[T]$.*

Proof. This uses the "restriction of scalars" idea. Since $\mathbb{C}[T]$ contains the field $\mathbb{C}$, we can restrict scalars and view M as a vector space over $\mathbb{C}$. Then M is finite dimensional. But $\mathbb{C}[T]$ is infinite dimensional over $\mathbb{C}$. So, $\mathbb{C}[T]$ cannot be a direct summand of M. So, it is torsion. Also, being finitely generated over the smaller ring means it is finitely generated over the bigger ring. □

By the structure theorem we now have:

$$M \cong \bigoplus \mathbb{C}[T]/(p_i(T)^{n_i})$$

where $p_i(T)$ is an irreducible polynomial. But $\mathbb{C}$ is *algebraically closed*. So, any polynomial has a root $a_i \in \mathbb{C}$ which means $T - a_i$ divides $p_i(T)$ which implies that

$$p_i(T) = T - a_i$$

up to multiplication by a scalar.

Lemma 10.2. *Let $p(T) = T - a$. Then the p-primary part of M is nonzero ($M_p \neq 0$) iff a is an eigenvalue of A.*

Proof. Suppose first that $x \in M = \mathbb{C}^n$ is an eigenvector of A with eigenvalue a. Then $x \neq 0$ and

$$Ax = ax$$

which means that

$$px = (A - a)x = 0.$$

This implies that x is p-primary. So, $x \in M_p$ making M_p nonzero.

Conversely, suppose that $M_p \neq 0$. Then there is an element $x \in M$ so that $ann(x) = (p^k)$. This means

$$p^k x = (A - a)^k x = 0$$

and

$$y = p^{k-1}x = (A - a)^{k-1}x \neq 0$$

But then

$$(A - a)y = 0$$

making $y \in M$ into an eigenvector of A with eigenvalue a. □

Since a is an eigenvalue, I started to write $a = \lambda$. Next I want to find a basis for the cyclic module $\mathbb{C}[T]/(p^k)$ where $p = T - \lambda$.

Lemma 10.3. *If $x \in M_p$ with $ann(x) = (p^k)$ then the cyclic module $Rx = \mathbb{C}[T]x = \mathbb{C}[A]x$ has basis*

$$y_1 = (A-\lambda)^{k-1}x, y_2 = (A-\lambda)^{k-2}x, \cdot, y_k = (A-\lambda)^0 x = x$$

as a vector space over $\mathbb{C}$.

Proof. The first point is to understand that if $ann(x) = (p^k)$ we mean that p^k is the *minimal polynomial* of A acting on x. In other words, $f(A)x = 0$ iff $p(T)^k | f(T)$. This means two things.

(1) $(A-\lambda)^k x = 0$
(2) If $f(T)$ is a nonzero polynomial of degree $< k$ then $f(A)x \neq 0$.

The second statement can be reinterpretted as saying that

$$x, Ax, A^2x, \cdots, A^{k-1}x \tag{10.1}$$

are linearly independent because any linear relation can be written as

$$\sum_{i=1}^{k} c_i A^{k-i} x = 0.$$

This says that $f(A)x = 0$ where $f(T) = c_1 T^{k-1} + \cdots + c_k$ is a polynomial of degree $k-1$ or less contradicting (2).

When (1) is expanded out it says that $A^k x$ is a linear combination of the vectors in (10.1). But then A^{k+1} is a linear combination of

$$A^k x, A^{k-1}x, \cdots, Ax$$

which is in the span of the vectors $A^{k-1}x, \cdots, x$ since A^k is in that span. So, the vectors in (10.1) for a basis for the cyclic module Rx.

This is not quite what we want. However, we can modify the basis above in the following way. Suppose that $f_i(T)$ is a polynomial of degree exactly equal to i and $f_0(T) = c$ is a nonzero constant. Then

$$f_0(A)x, f_1(A)x, \cdots, f_{k-1}(A)x$$

also forms a basis for Rx since they have the same span (by induction on k): the last vector $f_{k-1}(A)x$ is equal to a nonzero constant times $A^{k-1}x$ plus lower terms. But the lower terms are in the span of $A^i x$ for $i < k-1$ by induction. So, we get everything.

Since $f_i(T) = (T-\lambda)^i$ has degree i, we conclude that $(T-\lambda)^i x$ form a basis for Rx as claimed. □

10.3. **the Jordan canonical form for A.**

Lemma 10.4. *If $ann(x) = (p^k)$ where $p = T - \lambda$ then the matrix of A operating on the k-dimensional vector space Rx with respect to the basis given by the above lemma is equal to the $k \times k$ Jordan block with diagonal entries λ.*

Proof. The basis elements $y_i = (A-\lambda)^{k-i}x$ are related by the equation

$$y_{i-1} = (A-\lambda)y_i.$$

In other words,

$$Ay_i = \lambda y_i + y_{i-1}$$

and $Ay_1 = \lambda y_1$. Since the jth column of the matrix for A is the vector Ay_j written in terms of the basis $y_1, \cdots, y_k$, the matrix is

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}$$

This is the Jordan block $[\lambda]^k$. □

Finally, I recalled how matrices behave with respect to change of basis. To make it really clear, let me first do the 2×2 case.

Suppose that $n = k = 2$ and $y_1 = (A-\lambda)x$ and $y_2 = x$. Then $Ay_1 = \lambda y_1$ and $Ay_2 = \lambda y_2 + y_1$. This can be written as the matrix formula

$$A(y_1, y_2) = (Ay_1, Ay_2) = (y_1, y_2)\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

If we write $B = (y_1, y_2. \cdots)$ for the matrix with columns the basis elements y_1, y_2, etc. we get

$$AB = BJ$$

where J is the Jordan matrix. The fundamental theorem for modules over PID's gives

$$M \cong \bigoplus \mathbb{C}[T]/((T-\lambda_i)^{k_i})$$

By the lemmas above, this implies the following.

Theorem 10.5. *After conjugating by a basis change matrix B, any $n \times n$ complex matrix A is conjugate to a matrix in Jordan canonical form:*

$$B^{-1}AB = J = \bigoplus [\lambda_i]^{k_i}.$$

We need the uniqueness part of the fundamental theorem to tell us that the pairs (λ_i, k_i) are uniquely determined.